

RECEIVED  
CENTRAL FAX CENTER

JUN 30 2004

CLAIM AMENDMENTS AND LISTING

1

2 What is claimed is:

3 Claim 1. (currently amended) A method for generating a key pair  
4 for use in a digital signature scheme, the method comprising:5 - forming a private key which includes at least one  
6 enhancing key; and  
7 - forming a public key which includes a commitment to said  
8 at least one enhancing key, wherein the public key and the  
9 private key form the key pair; and  
10 - employing said key pair and said enhancing key in the  
11 generation of a digital signature.12 Claim 2. (Original) The method as recited in Claim 1, wherein the  
13 step of forming a public key comprises computing a function on a  
14 commitment to an enhancing key and a 1-time public key.15 Claim 3. (Original) The method as recited in Claim 1, wherein the  
16 enhancing key is randomly chosen.17 Claim 4. (Original) The method as recited in Claim 1, further  
18 comprising employing the enhancing key in a process.19 Claim 5. (Original) A method as recited as in Claim 4, wherein  
20 the process performs a hash calculation.21 Claim 6. (Original) A method as recited in Claim 1, further  
22 comprising computing a certificate for the public key.

DOCKET NUMBER: YOR919990229US2

-2/15-

1      Claim 7. (Original) A method as recited as in Claim 1, wherein  
2      the commitment is a TCR commitment.

3      Claim 8. (Original) The method as recited in Claim 7, further  
4      comprising employing the enhancing key in a process.

5      Claim 9. (Original) A computer program product comprising a  
6      computer usable medium having computer readable program code  
7      means embodied therein for generating a key pair, the computer  
8      readable program code means in said computer program product  
9      comprising computer readable program code means for causing a  
10     computer to effect the steps of claim 1.

11     Claim 10. (currently amended) A method of forming a TCR  
12     commitment in a digital signature scheme comprising:  
13         - providing a commitment for a first string, and  
14         - applying a TCR function to a second string that includes the  
15     commitment; and  
16         - employing said TCR commitment in the digital signature  
17     scheme.

18     Claim 11. (Original) A method as recited in Claim 10, wherein the  
19     step of applying includes:  
20         - choosing a random key for the TCR function.  
21         - evaluating the TCR function on the random key and the second  
22     string.

23     Claim 12. (Original) A method as recited in Claim 11, wherein the  
24     TCR function is a basic cryptographic primitive.

25     Claim 13. (Original) A method as recited in Claim 12, wherein the  
26     cryptographic primitive is the SHA-1 compress function.

1       Claim 14. (Original) A method as recited in Claim 10, wherein the  
2       step of applying forms a TCR function output which is 80 bits  
3       long.

4       Claim 15. (Original) An article of manufacture comprising a  
5       computer usable medium having computer readable program code  
6       means embodied therein for generating a key pair, the computer  
7       readable program code means in said article of manufacture  
8       comprising computer readable program code means for causing a  
9       computer to effect the steps of claim 1.

10      Claim 16. (Original) A method as recited in Claim 10, further  
11      comprising employing the TCR commitment in an enhanced commitment  
12      based signature scheme.

13      Claim 17. (Original) A method as recited in Claim 1, wherein the  
14      public-private key pair is used a bounded number of times.

15      Claim 18. (Original) A method as recited in Claim 17, where the  
16      bounded number is 36.

17      Claim 19. (Original) A method as recited in Claim 12, wherein the  
18      TCR function is a TCR hash tree based on a basic cryptographic  
19      primitive.

20      Claim 20. (Original) A method as recited in Claim 1, further  
21      comprising employing the key pair in a commitment based signature  
22      scheme.

23      Claim 21. (Original) The method as recited in Claim 4, wherein  
24      the process is a 36-time signature scheme.

-4/15-

DOCKET NUMBER: Y0R919990229US2

PAGE 4/15 \* RCVD AT 6/30/2004 12:45:07 PM [Eastern Daylight Time] \* SVR:USPTO-EFXRF-1/0 \* DNI:8729306 \* CSID:9149453281 \* DURATION (mm:ss):03:54

1       Claim 22. (Original) A method as recited in Claim 10, further  
2       comprising employing the TCR commitment in an E-commerce  
3       protocol.

4       23. (currently amended) A method for generating a TCR commitment  
5       opening function, said method comprising:

6       generating a TCR commitment opening function for extracting a  
7       data string committed to by at least one TCR commitment message,

8       utilizing a corresponding TCR opening string for each said at  
9       least one TCR commitment message, and

10       wherein the step of generating the TCR commitment opening  
11       function includes:

12               receiving a TCR commitment message and the corresponding TCR  
13               opening string;

14               extracting a hash value and a key from said TCR commitment  
15               message; and

16               extracting a regular opening string and a regular commitment  
17               message from said corresponding TCR opening string,

18               computing the TCR hash function with said key and said  
19               regular commitment message forming a result value, and

20               comparing said result value with said hash value;

21       if the step of comparing results in a compare, applying said  
22       regular opening commitment function on said regular opening

1 string and said regular commitment message to produce said data  
2 string.

3 Claim 24. (Original) An article of manufacture comprising a  
4 computer usable medium having computer readable program code  
5 means embodied therein for generating a TCR commitment opening  
6 function for extracting a data string committed to by at least  
7 one TCR commitment message, the computer readable program code  
8 means in said article of manufacture comprising computer readable  
9 program code means for causing a computer to effect the steps of  
10 claim 23.

11 Claim 25. (Original) A computer program product comprising a  
12 computer usable medium having computer readable program code  
13 means embodied therein for causing generation of a TCR commitment  
14 opening function, the computer readable program code means in  
15 said computer program product comprising computer readable  
16 program code means for causing a computer to effect the steps of  
17 claim 23.

18 Claim 26. (Previously amended) A method as recited in Claim 10,  
19 wherein the step of generating the TCR commitment function  
20 includes:

21 receiving a data string to be committed and receiving secret  
22 information, if any, in a regular commitment scheme;

23 computing a regular commitment message using said regular  
24 commitment scheme upon both said data string and said secret  
25 information;

26 randomly selecting a key for said TCR function;

1 computing said TCR function on said key and said regular  
2 commitment message and obtaining a resulting hash value;

3 forming a TCR commitment message including said resulting  
4 hash value and said key, said TCR commitment message being an  
5 output of said TCR commitment function.

6 Claim 27. (Original) A method as recited in Claim 26, further  
7 comprising saving said regular commitment message.

8 Claim 28. (Original) A method as recited in Claim 27, wherein the  
9 step of saving is performed for a commiter.

10 Claim 29. (currently amended) A method used in formation of a  
11 digital signature, the method comprising:

12 generating a TCR de-commitment function for de-committing at  
13 least one TCR commitment message employing a TCR function and a  
14 regular commitment scheme used in generating said at least one  
15 TCR commitment message, said TCR de-commitment function used in  
16 formation of the digital signature.

17 Claim 30. (Original) A method as recited in Claim 29, wherein the  
18 step of generating the TCR de-commitment function includes:

19 receiving a data string committed and receiving secret  
20 information used in generating said at least one TCR commitment  
21 message if any;

22 receiving a regular commitment message computed as part of  
23 generation of said at least one TCR commitment message;

-7/15-

DOCKET NUMBER: YOR919990229US2

PAGE 7/15 \* RCVD AT 6/30/2004 12:45:07 PM (Eastern Daylight Time) \* SVR:USPTO-EFXRF-1/0 \* DNI:8729306 \* CSID:9149453281 \* DURATION (mm:ss):03:54

1 computing the regular de-commitment function on using said  
2 regular commitment message, said data string and said secret  
3 information and generating a regular opening string;

4 forming a TCR opening string including said regular opening  
5 string and said regular commitment message, said TCR opening  
6 string being an output of said TCR de-commitment function.

7 Claim 31. (currently amended) A method for generating a function  
8 used in a digital signature scheme, said method comprising:

9 generating a TCR commitment function by employing a TCR function  
10 and utilizing a regular commitment scheme; wherein the step of  
11 generating the TCR commitment function includes:

12 receiving a data string to be committed and receiving secret  
13 information, if any, in said regular commitment scheme;

14 computing a regular commitment message using said regular  
15 commitment scheme upon both said data string and said secret  
16 information;

17 randomly selecting a key for said TCR function;

18 computing said TCR function on said key and said regular  
19 commitment message and obtaining a resulting hash value;

20 forming a TCR commitment message including said resulting  
21 hash value and said key, said TCR commitment message being an  
22 output of said TCR commitment function.

23 Claim 32. (Canceled)

1       33. (Previously amended) The method as recited claim 23 wherein  
2       reporting an error if the step of comparing results in a  
3       non-compare, and reporting a non-error if the step of comparing  
4       results in a compare.

5       Claim 34. (Canceled)

6       Claim 35. (currently amended) A method for use in a digital  
7       signature scheme, said method comprising:

8               constructing a TCR commitment scheme comprising:

9               a TCR commitment function;  
10              a TCR de-commitment function; and  
11              a TCR commitment opening function,

12             by employing a TCR function and a regular commitment scheme,  
13             wherein the step of constructing the TCR commitment function  
14             includes:

15             receiving a data string to be committed and receiving secret  
16             information if any in said regular commitment scheme;

17             computing a regular commitment message using said regular  
18             commitment scheme upon both said data string and said secret  
19             information;

20             randomly selecting a key for said TCR function;

21             computing said TCR function on said key and said regular  
22             commitment message and obtaining a resulting hash value; and

1 forming a TCR commitment message including said resulting  
2 hash value and said key, said TCR commitment message being an  
3 output of said TCR commitment function.

4 Claim 36. (Original) An article of manufacture comprising a  
5 computer usable medium having computer readable program code  
6 means embodied therein for generating a TCR commitment function,  
7 the computer readable program code means in said article of  
8 manufacture comprising computer readable program code means for  
9 causing a computer to effect the step of claim 25.

10 Claim 37. (Original) A method as recited in Claim 25, wherein the  
11 TCR function is a basic cryptographic primitive.

12 Claim 38. (Original) A method as recited in Claim 37, wherein the  
13 cryptographic primitive is the SHA-1 compress function.

14 Claim 39. (Original) A method as recited in Claim 26, wherein  
15 said resulting hash value is 80 bits long.

16 Claim 40. (Original) A method as recited in Claim 25, wherein the  
17 TCR function is a TCR hash tree based on a basic cryptographic  
18 primitive.

19 Claim 41. (Original) A method as recited in Claim 35, further  
20 comprising employing the TCR commitment scheme in an enhanced  
21 commitment based signature scheme.

22 Claim 42. (Original) A method as recited in Claim 35, further  
23 comprising employing the TCR commitment scheme in an E-commerce  
24 protocol.

-10/15-

DOCKET NUMBER: YOR919990229US2

1       Claim 43. (Previously amended) An article of manufacture  
2       comprising a computer usable medium having computer readable  
3       program code means embodied therein for causing formation of a  
4       TCR commitment message, the computer readable program code means  
5       in said article of manufacture comprising computer readable  
6       program code means for causing a computer to effect the steps of  
7       claim 31.

8       Claim 44. (Original) An article of manufacture comprising a  
9       computer usable medium having computer readable program code  
10       means embodied therein for generating a TCR de-commitment  
11       function, the computer readable program code means in said  
12       article of manufacture comprising computer readable program code  
13       means for causing a computer to effect the steps of claim 29.

14       Claim 45. (new) A method for generating a key pair, the method  
15       comprising:

16               - forming a private key which includes at least one  
17               enhancing key; and  
18               - forming a public key which includes a commitment to said  
19               at least one enhancing key, wherein the public key and the  
20               private key form the key pair.

21       Claim 46. (new) A method of forming a TCR commitment comprising:  
22               - providing a commitment for a first string, and  
23               - applying a TCR function to a second string that includes the  
24               commitment.

25       Claim 47. (new) A method comprising:

-11/15-

DOCKET NUMBER: Y0R919990229US2

PAGE 11/15 \* RCV'D AT 6/30/2004 12:45:07 PM [Eastern Daylight Time] \* SVR:USPTO-EFXRF-1/0 \* DNIS:8729306 \* CSID:9149453281 \* DURATION (mm:ss):03:54

1 generating a TCR de-commitment function for de-committing at  
2 least one TCR commitment message employing a TCR function and a  
3 regular commitment scheme used in generating said at least one  
4 TCR commitment message.

DOCKET NUMBER: YOR919990229US2

-12/15-

PAGE 12/15 \* RCV'D AT 6/30/2004 12:45:07 PM [Eastern Daylight Time] \* SVR:USPTO-EFXRF-1/0 \* DNIS:8729306 \* CSID:9149453281 \* DURATION (mm:ss):03:54